De Trusted Third Party bestaat niet

Koops, E.J.

Published in:
Informatie : Maandblad voor de Informatievoorziening

Publication date:
1999

Koops, B.J. (1999). ‘De Trusted Third Party bestaat niet’, Verschenen in: *Informatie 41* (december), 40-41

De Trusted Third Party bestaat niet

Bert-Jaap Koops

Trusted Third Parties zijn in. Je kunt geen beleidsdocument over e-handel lezen, of je struikelt over de term. Twee van de belangrijkste voorwaarden voor het opbloeien van e-handel zijn immers veiligheid en vertrouwen, en de Trusted Third Party wordt door menigeen gezien als een wondermiddel om beide te bewerkstelligen. Een TTP is een vertrouwde, onafhankelijke organisatie die diensten aanbiedt die de betrouwbaarheid van elektronische gegevensuitwisseling en gegevensopslag vergroten. In een mondiale netwerkomgeving waarin iedereen met iedereen lijkt te willen handelen, is zo’n TTP bij uitstek geschikt het vertrouwen tussen onbekende partijen te bewerkstelligen. Er is alleen één probleem. De Trusted Third Party bestaat niet.

Voor het beveiligen van elektronische gegevensuitwisseling en -opslag is een veelheid aan maatregelen vereist - zowel technische, organisatorische als juridische. Techniek, waarbij cryptografie een vooraanstaande rol speelt, is op zichzelf niet genoeg. Voor authenticatie met een cryptografische digitale handtekening is er immers zekerheid nodig dat de privésleutel waarmee de handtekening is gezet, ook daadwerkelijk toebehoort aan de afzender - iedereen kan wel een cryptosleutelpaar met de naam Loesje Handelaar genereren. Hier komt de organisatorische maatregel van de TTP om de hoek kijken: een onafhankelijke partij die de binding tussen sleutel en persoon garandeert in een digitaal certificaat. En om te verzekeren dat de TTP goed doet wat hij moet doen, kan de overheid juridische maatregelen treffen, zoals het stellen van randvoorwaarden voor TTP’s. De Nederlandse overheid heeft daartoe in juni een notitie “Nationaal TTP-project” aan de Tweede Kamer aangeboden. De bedoeling is dat - grotendeels door marktwerking - een betrouwbare TTP-infrastructuur wordt opgezet die de veiligheid van de e-handel zal waarborgen. Het notariaat hoopt daar een graantje van mee te pikken en stofte onlangs zijn imago af met de lancering van DigiNotar, een club van TTP-notarissen.

Maar is de TTP wel het wondermiddel dat hij lijkt te zijn? Ik vraag me dat af. Ten eerste bestaat er niet zoiets als *de* Trusted Third Party. Diverse diensten kunnen de betrouwbaarheid van e-handel faciliteren, maar deze diensten lopen nogal uiteen. Het garanderen van de binding tussen een cryptosleutelpaar en een persoon wordt gedaan door een Certificatie-Autoriteit (CA). Deze vervult meestal ook de functies van Registratie-Autoriteit (die de identiteit van de aanvrager controleert voordat een certificaat wordt afgegeven) en van Certificaten-Aanbieder, een online databank waarin e-handelaars certificaten kunnen opzoeken en controleren op geldigheid. Onder de term TTP wordt echter vaak ook een instantie verstaan die cryptografische sleutels beheert en een sleutelherwinningsdienst aanbiedt tegen het risico van sleutelverlies (in het Engels *Key Escrow Agent* of *Key Recovery Agent* genaamd). Dat is een andersoortige TTP dan een CA, omdat het hier gaat om cryptografie die de vertrouwelijkheid, niet de authenticiteit en integriteit, van gegevens waarborgt. Het op één hoop gooien van deze twee is gevaarlijk, omdat het onverstandig is hetzelfde sleutelpaar te gebruiken voor zowel handtekeningen als voor vertrouwelijkheid. Als de overheid bij een opsporingsactie een privésleutel vordert om aangetroffen cijferteksten te kunnen ontsleutelen, is het niet handig als de betrokkene met dezelfde sleutel berichten ondertekent - de politie kan dan immers berichten vervalsen!
Ten slotte zijn er nog diensten die de bewijs- en bewaarfunctie van gegevens faciliteren. Te denken valt aan het tijdstempelen van berichten, het waarborgen van ontvangst- en verzendbewijzen, en het bewaren van documenten en certificaten om als bewijs te dienen in eventuele toekomstige geschillen.
Het op een hoop gooien van partijen die deze uiteenlopende diensten aanbieden in één koepelbegrip Trusted Third Party is misleidend, omdat het suggereert dat het vergelijkbare dienstaanbieders zijn, of - erger nog - dat het één organisatie is die al die diensten aanbiedt.

Koops, B.J. (1999). ‘De Trusted Third Party bestaat niet’, Verschenen in: *Informatie 41* (december), 40-41

Vanwege de substantiële verschillen tussen de diensten is dat discutabel. Er bestaat geen TTP, er zijn alleen CA’s, Sleutelbeheerinstanties en Bewijs- en Bewaar-Autoriteiten. Eigenlijk zijn er alleen CA’s, want andersoortige “TTP’s” zijn op de markt nog nauwelijks gesignaleerd.

Ten tweede bestaat er niet zoiets als een *Trusted* Third Party. Het opnemen van de term ‘trust’ in de naam is misleidend en aanmatigend, want het suggereert dat de TTP zelf vertrouwd is (logischer was ‘trustworthy’ - betrouwbaar - geweest). Maar volgens mij zit de ‘trust’ veeleer in het doel van de TTP: het vertrouwen in e-handel te verhogen. Je kunt je afvragen of je daar een derde partij voor nodig hebt. Er wordt nu ook al de nodige handel gedreven via het Internet, en we kennen ook al jaren het fenomeen van de telefonische en postorderbestelling. Moet daar een derde partij tussen, alleen omdat we het nu digitaal doen? Bovendien is het grootste risico in e-handel niet dat een partij niet is wie hij zegt te zijn, maar dat een partij niet doet wat hij beloofd heeft - leveren of betalen. Tegen dat risico helpt een TTP hoegenaamd niets. Kortom, men kan zich afvragen of een TTP wel nodig is voor het vertrouwen in e-handel.
Maar er is meer. Ik weet niet zeker of TTP’s zelf wel te vertrouwen zijn. Een goed criterium om dat te beoordelen is de aansprakelijkheid van de TTP: als het misgaat, kan ik hem dan aanspreken op de schade? Het blijkt dat CA’s tot nu toe grotendeels aansprakelijkheid uitsluiten. Dat is logisch, omdat het een nieuwe dienst betreft en de schade moeilijk te overzien valt; het is mogelijk dat een fout certificaat bij een miljoenentransactie tot grote schade leidt. Bij sleutelbeheerdiensten is de mogelijke schade nog onvoorspelbaarder en potentieel groter. Maar het grotendeels uitsluiten van aansprakelijkheid komt het vertrouwen in de CA of Sleutelbeheerder zelf niet ten goede. Ik raak niet bepaald onder de indruk van een bedrijf dat zegt: “Wij bieden u deze fantastische dienst voor een schappelijk prijsje. <kleine lettertjes>P.S. U moet zelf de schade betalen als het misgaat.</kleine lettertjes>”

Ten derde betwijfel ik ook of er wel zoiets bestaat als een Trusted *Third* Party. Het is immers een instantie die een dienst aanbiedt en die contracten sluit met afnemers van de dienst. Wie is dan de derde? Bedoeld is waarschijnlijk dat in het gegevensverkeer tussen twee partijen een TTP als een intermediair het onderlinge vertrouwen kan bewerkstelligen. Maar er zijn ook “TTP”-diensten die maar één partij betreffen, zoals een sleutelherwinningsdienst of het bewaren van documenten. Bovendien is in een situatie waarin een leverancier vertrouwt op het certificaat en dus de handtekening van een afnemer, het maar de vraag of de CA daarbij een derde is. Hij heeft immers een contract met de afnemer, niet met de leverancier. Dat betekent ook dat de CA zich tegenover de leverancier waarschijnlijk niet kan beroepen op de uitsluiting van aansprakelijkheid, die hij bij de afnemer heeft bedongen. Juridisch gesproken heet het dat de exoneratieclausule geen derdenwerking heeft. De TTP is dus in dit juridisch opzicht geen derde partij - laat staan een vertrouwde.
Ten slotte kan een TTP ook geen Trusted Third *Party* zijn, want een onafhankelijke intermediair mag per definitie geen partij kiezen.

Mijn conclusie luidt dan ook dat “de Trusted Third Party” niet bestaat. Er zijn misschien dienstaanbieders die de betrouwbaarheid van e-handel kunnen vergroten, maar laten we die gewoon bij hun naam noemen: Certificatie-Autoriteiten, Sleutelbeheerinstanties en Bewijs- en Bewaar-Autoriteiten. Vertrouwen zullen ze moeten afdwingen door de kwaliteit van hun diensten, niet door suggestieve naamgeving. En derden en partijen zijn ze ook al niet. Kortom, “TTP” is een draak van een term die ontleend is aan het Babylonisch, en die thuishoort in de vuilnisbak van onze taal.

Meer informatie
“Nationaal TTP-project”, Kamerstukken II, 1998-1999, 26 581, nr. 1, te vinden op WWW <http://www.minvenw.nl/dgtp/beleid/fr_beleid.htm>

Koops, B.J. (1999). ‘De Trusted Third Party bestaat niet’, Verschenen in: *Informatie 41* (december), 40-41

Dossier Trusted Third Parties, *Computerrecht* 1998 nr. 5, pp. 206-234, WWW <http://cwis.kub.nl/~frw/people/koops/pub/ttp-dos.htm>

Dossier E-Commerce, *Computerrecht* 1999 nr. 3, pp. 97-140

DigiNotar, WWW <http://www.diginotar.nl/>